IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of
Dent et al.

Serial No.: 09/862,879

Filed: May 22, 2001

For: **Security System**

Attorney's Docket No: 4015-844

Patent Pending

Examiner: David Y. Jung

Group Art Unit: 2134

Confirmation No.: 8844

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☒ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 273-8300.

November 7, 2005 — Date

Kathleen Koppen — Kathleen Koppen

11/15/2005 DTESSEM1 00000030 09862879

01 FC:1402 500.00 OP

APPEAL BRIEF

Dear Sir or Madam:

This Appeal Brief is being timely submitted. Applicants note that the due date for this Brief falls on Sunday, November 6, 2005. Therefore, mailing this Brief on Monday, November 7, 2005 is timely, and no extension of time fees should be due. A check in the amount of $500 is enclosed to cover the requisite fee pursuant to 37 C.F.R. §41.20. However, if there are any additional fees required, the Commissioner is authorized to charge Deposit Account No. 18-1167.

(I.) REAL PARTY IN INTEREST

The real party in interest is Ericsson Inc., the assignee of the present invention.

(II.) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Applicants' knowledge.

(III.) STATUS OF CLAIMS

A total of seventy-seven (77) claims numbered 1-77 have been presented for examination, all of which are pending. All claims 1-77 stand finally rejected by the Examiner. Accordingly, Applicants appeal the rejection of claims 1-77.

(IV.) STATUS OF AMENDMENTS

All amendments have been entered to the best of Applicants' knowledge.

(V.) SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a security system that provides security for a protected function such as unlocking a door. *Spec.*, pg. 2, ll. 5-6. Particularly, parties authorized to access the protected function may use a wireless communications device to communicate with an access control device that controls access to the protected function. *Spec.*, pg. 2, ll. 7-8. The access device sends an authentication challenge to which the wireless communications device generates and sends a response. The response is based on the authentication challenge received by the wireless communications device and an authentication code stored in its memory. The access control device checks the received response against an expected response stored in its memory. If the response is valid, the access control device allows the user to gain access to the protected function. *Spec.*, pg. 2, ll. 10-20.

Figure 2 illustrates one example of a wireless communications device configured according to one embodiment of the present invention. The wireless communications device (100) may be a BLUETOOTH equipped device, such as a cellular phone or a Personal Digital Assistant (PDA). *Spec.*, pg. 5, ll. 21-25; Figures 1, 3, 5. In one embodiment, the wireless

communications device receives an authorization code from a central controller (40) that may be communicatively connected to an access control device (20), such as an electronic door lock. *Spec.*, p. 4, ll. 4-6; Figures 1, 4-5. In another embodiment, the wireless communications device receives the authorization code from the access control device. The authorization code may be generated based on a master code stored in memory, such as a tamper resistant security module (e.g., a smart card). Figures 2-5, 110; *Spec.*, p. 4, ln. 18 – p. 5, ln. 4; p. 6, ll. 24; p. 9, ll. 15-24. To unlock a door, for example, the party uses the wireless communications device to transmit an access request to the door lock. The door lock responds to the request by transmitting an authentication challenge to the wireless communications device. *Spec.*, p. 4, ll. 6-9. The authentication challenge may include, for example, a random bit string or number that is not known to the wireless communications device *a priori*. *Spec.*, p. 4, ll. 9-11. Upon receipt of the challenge, the wireless communications device computes an authentication response by using a predetermined algorithm to combine selected portions of the authentication challenge with the authorization code received from the central controller. The wireless communications device then sends the generated response to the door lock. *Spec.*, p. 4, ll. 11-14.

The door lock also stores the authorization code in memory. *Spec.*, p. 4, ll. 22-25. The door lock computes an expected authentication response using the same combining algorithm that the wireless communications device used to compute its response to the authentication challenge. *Spec.*, p. 4, ll. 14-16. Alternatively, the central controller could compute the expected response and provide it to the door lock. *Spec.*, p. 12, ll. 3-5. Likewise, the central controller or the door lock can generate the authentication challenge. The door lock compares the authentication response received from the wireless communications device to the expected authentication response. If the two match, the door lock actuates an electronic locking mechanism to unlock the door for the user of the wireless communications device. *Spec.*, p. 4, ll. 16-17; p. 12, ll. 5-7.

The authorization code may be generated or computed based on a combination of a secret code and a time indication to limit access to a protected function to a defined time period. *Spec.*, p. 9, ll. 8-14. The authorization code may further be generated or computed by combining a device identifier associated with the access control device with the secret code and the time indication. *Spec.*, p. 9, ll. 15-24.

A plurality of authorization codes may be stored in memory, wherein each authorization code is associated with a different time period. *Spec.*, p. 11, ln. 19 – p. 12, ln. 2; p. 2, ll. 21-23. The wireless communications device may include a device identifier associated with the access control device in the access request to the access control device. *Spec.*, p. 11, ll. 5-8. The wireless communications may also include a group identifier derived from the device identifier in the access request transmitted to the access control device. *Spec.*, p. 11, ll. 8-9.

Computing the authorization response may be accomplished, for example, by combining selected portions of the authentication challenge and the authorization code with a non-reversible function. The selected portions of the authentication challenge may be, for example, a random number and/or a device identifier associated with the access control device. *Spec.*, p. 14, ln. 8-11.

The wireless communications device may transmit an electronic identity to a central controller, and receive the authorization code once the central controller has verified the electronic identity. The electronic identity may be, for example, a credit identity of a user verified by a credit agency. *Spec.*, p. 10, ln. 1-20.

(VI.) GROUNDS OF REJECTION

The Examiner finally rejected claims 1-4, 6-11, 15-35, 40-50, 54-56, and 60-71 under 35 U.S.C. § 103(a) as being unpatentable over the patent to Henderson (U.S. Patent No. 5,602,536, hereinafter "Henderson").

The Examiner also finally rejected claims 5, 12-14, 51-53, and 57-59 under 35 U.S.C. § 103(a) as being unpatentable over Henderson in view of the patent to Wang (U.S. Patent No. 6,175,922, hereinafter "Wang").

The Examiner also finally rejected claims 36-39 and 72-77 under 35 U.S.C. § 103(a) as being unpatentable over Wang.

(VII.) ARGUMENT

A. The patent to Henderson does not render claim 1 obvious under §103.

Claim 1 is directed to a method of enabling or activating a protected function. In claim 1, a wireless communications device computes an authentication response for transmission to an access control device. The requisite computation is based on an authentication challenge received from the access control device and an authorization code stored in memory of the wireless communications device. For the Board's convenience, claim 1 appears below in its entirety.

> 1. A method of enabling or activating a protected function, said method comprising:
>
> storing an authorization code in a wireless communication device;
>
> transmitting an access request from said wireless communication device to an access control device;
>
> receiving an authentication challenge from said access control device at said wireless communication device in response to said access request;
>
> computing an authentication response based on said authentication challenge and said authorization code; and
>
> transmitting said authentication response from said wireless communication device to said access control device.

The Examiner contends that the Henderson patent computes an authentication response. It does not. Henderson teaches a real estate lockbox system comprising a lockbox (12), an electronic key (14), and a computer (18). *Henderson*, Figure 1. A real estate agent may use the electronic key to open the lockbox and gain access to a door key contained inside the lockbox. *Henderson*, col. 3, ln. 62 – col. 4, ln. 7. In operation, the electronic key sends an

interrogation signal to the lockbox to "wake-up" the lockbox. In response, the lockbox returns a signal to the electronic key that includes battery and date information stored at the lockbox. The electronic key then compares an expiration date stored in its memory to the date received from the lockbox. If the comparison reveals that the date stored in the electronic memory has not expired, the electronic key sends information identifying the agent, the agency, the real estate board, and "permission codes" to the lockbox. The lockbox compares this received information to data stored in its memory and, if valid, allows the real estate agent to access the key contained within the lockbox. *Henderson*, col. 23, ln.65 – col. 24, ln. 31.

The electronic key of Henderson does not compute an authentication response based on an authentication challenge received from the lockbox and an authentication code. Rather, it simply sends a signal back to the lockbox that contains predetermined information already stored in memory. *Henderson*, col. 24, ll. 13-15; col. 6, ln. 59 – col. 7, ln. 15. The electronic key does not perform any computations on battery and date information received from the lockbox, nor does the electronic perform computations on its stored information prior to sending it to the lockbox. Henderson discloses only that the electronic key reads information from its memory in response to receiving a signal from the lockbox, and sends the information *as is* to the lockbox. Indeed, the simplistic act of responding to a received signal with predetermined information already stored in memory does not teach, or even suggest the complexities of computing an authentication response based on a received authentication challenge and an authentication code.

Moreover, it is impossible for the electronic key of Henderson to teach or suggest the computations needed to compute the authentication response of claim 1. The Examiner's own admission undergirds this fact. Particularly, the Examiner readily admits that Henderson does not teach or suggest an authentication challenge "in the sense of the claim." *Final Office Action*, page 3, ¶ 3. However, claim 1 requires computing the authentication response at least partially on the received authentication challenge. It is impossible for the electronic key of Henderson to

compute the claimed authentication response if the lockbox never sends, and the electronic key never receives, an authentication challenge "in the sense of the claim" (i.e., the required authentication challenge).

The Examiner attempts to remedy this deficiency of the Henderson reference by contemplating that authentication challenges for the purpose of security are well-known in "advanced systems." The Examiner notes passwords in computers and long distance phone cards as examples of such "advanced systems." *Final Office Action*, pp. 3-4. The Examiner alleges that because these "advanced systems" are purportedly known to use authentication challenges, it would be obvious to use them in the claimed invention. There are at least three reasons why the Board should disregard this contention.

First, the Henderson patent teaches a method of gaining access to a real estate lockbox to obtain a door key. Real estate lockbox systems are completely unrelated to passwords in computers or long-distance phone cards. One has nothing to do with the other, and one skilled in the art would not be motivated to look to the computer password or long-distance phone card arts to modify the operations of a real estate lockbox system.

Second, the Examiner's contention says only that passwords for computers and long-distance phone cards *in general* teach authentication challenges. However, even if these contemplated "advanced systems" do exist, and even if they do use authentication challenges, the Office Action is devoid of any evidence whatsoever of what such a system might be. That is, the Examiner never specifies any particular system, and does not attempt to prove that passwords for computers and long-distance phone cards can be used to gain access to the real estate lockbox of Henderson. Henderson certainly does not suggest that the disclosed lockbox system could be modified to use password or long-distance phone card functionality.

Third, modifying the lockbox system as the Examiner suggests does not produce an electronic key that computes an authentication response as required by claim 1. Specifically, both "advanced systems" noted by the Examiner are well-known to operate based on

predetermined data. A computer, for example, prompts a user to enter a known password. The user does not compute the password based on the computer prompt, but rather enters the exact pre-determined key sequence using a keyboard. Likewise, long-distance phone cards are pre-programmed with information prior to sale. Long-distance phone cards do not compute an authentication response using a received authentication challenge and an authentication code. Rather, a card reader reads the pre-programmed data stored from the card's magnetic strip.

Simply put, the Examiner's alleged motivation to modify Henderson is unsupported by Henderson. It is a conclusory statement that because computer passwords and long-distance phone cards allegedly use authentication challenges for security, it would be obvious to use them in Henderson. The Henderson patent does not support this allegation, and the Examiner never attempts to prove that it does. In fact, the Examiner never offers anything other than an unsubstantiated assertion. A simple conclusory statement based on subjective belief and unknown authority is not now, and has never been, a legally sufficient motivation to modify a reference. The law requires the Examiner to specifically point out the rationale behind the motivation, and further, base the rationale on concrete evidence of record. Anything less is legal error.

> [The] factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority...Thus, the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion.

In re Lee, 61 U.S.P.Q. 2d 1430,1434 (Fed. Cir. 2002) (emphasis added).

Therefore, Henderson fails to teach or suggest claim 1, and Henderson cannot be modified as the Examiner asserts. In addition, whatever motivation the Examiner provides to modify Henderson is left wanting for legal support. Accordingly, the §103 rejection of claim 1 fails as a matter of law.

B. The patent to Henderson does not render claim 40 obvious under §103.

Claim 40 is directed to a device for enabling or activating a protected function. In claim 40, the device includes a processor that computes an authentication response for transmission to an access control device. The processor computes the authentication response based on an authentication challenge received from the access control device and an authorization code stored in its memory. For the Board's convenience, claim 40 appears below in its entirety.

> 40. A device for enabling or activating a protected function, said device comprising:
> memory to store an authorization code;
> a wireless transmitter to transmit an access request and an authentication response to an access control device;
> a wireless receiver to receive an authentication challenge from said access control device responsive to said access request;
> a processor to compute said authentication response based on said authentication challenge received from said access control device and said authorization code.

The electronic key of Henderson has a CPU and memory, but the CPU does not compute an authentication response based on a received authentication challenge and an authentication code stored in the memory. The electronic key memory stores only values. The electronic key CPU simply reads those values from memory responsive to receiving the lockbox signal, and sends those values to the lockbox. *Henderson*, col. 24, ll. 13-20; col. 6, ln. 59 – col. 7, ln. 15. The electronic key CPU does not compute a response based on the information received from the lockbox. It does not change or alter the values prior to sending them to the lockbox. A CPU that merely responds with predetermined information does not teach or suggest computing an authentication response based on a received authentication challenge and an authentication code stored in memory. Indeed, the electronic key CPU cannot compute the claimed authentication response based on data the Examiner admits it never receives.

Applicant respectfully notes that the Examiner supports the rejection of claim 40 with the same legally insufficient reasons as those stated above for claim 1. The Examiner simply states that Henderson could be modified to have an authentication challenge for the motivation of

security. However, the Federal Circuit has consistently held that simply because a reference could be modified does not mean there is motivation to do so. *In re Laskowski*, 871 F.2d 115, 117 (Fed. Cir. 1989); *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984). Henderson does not support the theory that it could be modified using computer passwords or long-distance phone cards. And, as stated above, the Examiner never attempts to support the assertion. Therefore, the motivation to modify Henderson with respect to claim 40 fails for the same reasons as those stated above with respect to claim 1.

Henderson does not teach or suggest claim 40. Nor can Henderson be modified as the Examiner asserts to render claim 40 obvious. Additionally, the proffered motivation is legally insufficient. Therefore, the §103 rejection of claim 40 fails as a matter of law.

C. The patent to Henderson does not render claim 15 obvious under §103.

Claim 15 is directed to a method of enabling or activating a protected function. Claim 15 requires transmitting an authentication challenge that a wireless communication device receiving the challenge uses to compute a response. The access control device of claim 15 also compares the received authentication response with an expected authentication response. Because access to the protected function depends on whether these two match, the expected authentication response is also necessarily based in part on the claimed authentication challenge. For the Board's convenience, claim 15 appears below in its entirety.

15. A method of enabling or activating a protected function, said method comprising:
    receiving an access request from a wireless communication device at an access control device;
    transmitting an authentication challenge from said access control device to said wireless communication device in response to said access request;
    receiving an authentication response based on said authentication challenge and an authorization code;
    comparing said received authentication response with an expected authentication response; and
    generating a control signal to permit access to said protected function if said received authentication response matches said expected authentication response.

The Examiner admits that Henderson fails to teach or suggest the claimed authentication challenge, but dismisses this deficiency out of hand by asserting that Henderson only fails to teach or suggest an authentication challenge "in the sense of the claim." However, the authentication challenge of claim 15 is by definition necessarily claimed "in the sense of the claim." Thus, if the Henderson patent does not teach an authentication challenge "in the sense of the claim," then it necessarily fails to teach or suggest the claimed authentication challenge. That is, the Henderson lockbox cannot transmit the claimed authentication challenge, receive a response based in part on the claimed authentication challenge, or compare a received authentication response against an expected authentication response that is itself based on the claimed authentication challenge. Indeed, because Henderson does not teach or suggest the authentication response "in the sense of the claim," Henderson cannot teach or suggest any element of claim 15 that includes the authentication challenge.

The lockbox of Henderson does not transmit an authentication challenge to the electronic key of Henderson. Rather, it simply sends a signal that includes lockbox battery information and a date. This is not an authentication challenge, nor would anyone skilled in the art understand it to be an authentication challenge. In contrast, it is information that the electronic key uses to determine whether it should or should not return predetermined values stored in its memory. *Henderson*, col. 24, ll. 5-12.

Further, Henderson does not compare an authentication response to an expected authentication response. Rather, the Henderson lockbox compares predetermined values stored in its memory to the predetermined values received from the electronic key. Those received values simply identify the real estate agent, the agency, and the real estate board. These values are not based on the lockbox battery information or the expiration date transmitted by the lockbox. Nor are they part of any information sent by the lockbox to the electronic key. Rather, they are independent of this data. As such, whatever response the lockbox receives cannot be based in part on an authentication challenge sent by the lockbox.

Further, the Examiner proffers the same legally insufficient motivation for claim 15 as offered for claim 1. However, for the reasons stated above, the Examiner's attempted corollary between the claimed authentication challenge and the alleged use of authentication challenges in unspecified computer password systems and long-distance phone cards also fails scrutiny.

As such, Henderson does not teach or suggest claim 15. Nor can it be modified as the Examiner contends to render claim 15 obvious. In addition, the Examiner's motivation to modify Henderson fails legal scrutiny. Accordingly, the §103 rejection of claim 15 fails as a matter of law.

D. The patent to Henderson does not render claim 60 obvious under §103.

Claim 60 is directed to access control device that secures a protected function. In claim 60, the access control device comprises a processor configured to generate an authentication challenge responsive to an access request from a wireless communications device, transmit the authentication challenge to the wireless communications device, receive an authentication response from the wireless communications device, and compare the received authentication response to an expected authentication response stored in memory of the access control device. For the Board's convenience, claim 60 appears below in its entirety.

60. An access control device to secure a protected function, said access control device comprising:
    a wireless transceiver to communicate with a wireless communication device;
    a processor programmed to:
        generate an authentication challenge in response to an access request from said wireless communication device;
        transmit said authentication response via said wireless transceiver to said wireless communication device;
        receive an authentication response from said wireless communication device via said wireless transceiver;
        compare said received authentication response to an expected authentication response based on said authentication challenge and an authorization code; and
        generate a control signal to permit access to said protected function if said expected authentication response matches said received authentication response.

The Henderson lockbox includes a CPU. However, for the reasons stated above, Henderson does not teach or suggest the claimed authentication challenge. Because Henderson does not teach or suggest the claimed authentication challenge, Henderson necessarily cannot teach or suggest the claimed processor. Indeed, the lockbox CPU of Henderson simply sends battery condition information and an expiration date stored in its memory. The lockbox CPU further receives information from the electronic key, and compares it to values stored in its memory; however, the values against which the lockbox CPU compares the received information are themselves predetermined and stored in lockbox memory. *Henderson*, col. 5, ll. 32-37; col. 24, ll. 21-23. Henderson does not compare the received values against an expected authentication response that is based on an authentication challenge and an authentication code. In fact, because Henderson fails to teach or suggest the authentication challenge, it necessarily fails to teach or suggest the claimed processor.

Therefore, Henderson does not teach or suggest claim 60. Nor can Henderson be modified to render claim 60 obvious as the Examiner contends. Moreover, the proffered motivation to modify Henderson is the same as that provided for claim 1, and thus, is *legally insufficient* for reasons similar to those provided above.

E. The patent to Wang does not render claim 36 obvious under §103.

Claim 36 is directed to a method of programming a wireless communication device with an authorization code used to enable or activate a protected function. Claim 36 is directed to a central controller that computes an authentication code from a master code stored in its memory responsive to an initialization request received from a wireless communications device. The central controller provides the wireless communications device with the authentication code. For the Board's convenience, claim 36 appears below in its entirety.

> 36. A method of programming a wireless communication device with an authorization code used to enable or activate a protected function, said method comprising:
> storing a master code in a central controller;
> receiving an initialization request from said wireless communication device;
> computing an authorization code based on said master code at said central controller in response to receipt of said initialization request;
> communicating said authorization code to said wireless communication device.

Wang discloses a system that is used for approving electronic transaction requests. *Wang*, col. 1, ll. 10-16. Systems that might use the Wang method are those that facilitate merchant-consumer transactions, such as ATM machines and Point-of-Sale (POS) systems. *Wang*, col. 18, ln. 33 – col. 19, ln. 17. In Wang, a user's Portable Electronic Authorization Device (PEAD) (906, 908) receives an executable transaction program (TP) from a server (902) via a communications network. *Wang*, Figures 9A-9B; col. 14, ln. 63 – col. 15, ln. 39. Once downloaded, the user may use the PEAD to approve an electronic transaction.

The TP of Wang is not an authorization code, but an executable computer program that carries out the steps required to perform the electronic transaction. *Wang*, col. 15, ll. 1-18. According to Wang, the TP may download data pertaining to items or goods or services that the user wants to purchase, such as an appliance or securities. *Wang*, col. 15, ll. 47-57. The TP also permits the user to enter various data regarding the transaction, indicate approval of the transaction, and encrypt transaction data upon approval of a transaction. *Wang*, col. 15, ll. 58-

63. In cases where the TP resides on a device separate from the PEAD, the TP contains codes that allow it to search for a PEAD automatically. *Wang*, col. 16, ll. 7-19.

The TP of Wang is far from being an authentication code. It is an executable computer program that performs predetermined functionality. The TP des not contain an authorization code computed from a master code stored at the server, nor does Wang ever suggest that it does. Moreover, Wang does not teach or suggest that the server computes an authorization code for transmission to a user's wireless communications device. In fact, Wang never teaches or suggests that the server stores a master code in its memory. Applicants respectfully note that the Office Actions are conspicuously devoid of any evidence to the contrary. The Examiner relies only upon the "Brief Summary" section of Wang that describes functionality in broad, sweeping language. Yet, even this section fails to support the Examiner's assertions.

Further, the Examiner admits that Wang does not teach or suggest initialization "in the sense of the claim." *Final Office Action*, p. 5, ¶2. However, this admission necessarily means that Wang cannot teach or suggest claim 36. Particularly, the initialization in claim 36 is an initialization request. The receipt of the initialization request causes the central controller to compute the claimed authentication code. If Wang does not teach initialization "in the sense of the claim," then Wang necessarily fails to teach or suggest that a server computes the authorization code responsive to receiving the initialization request.

In addition, the Examiner has failed to put forth a *legally sufficient* motivation to modify Wang. The Examiner states that Wang teaches a series of on-going transactions and that initialization situations among transactions are well-known. Therefore, the Examiner theorizes that it would be obvious to one skilled in the art to modify Wang to include an "initialization" situation for efficiency and security. This alleged motivation is conclusory. The Examiner never attempts to describe how the Wang system might incorporate these alleged well-known initialization situations. Nor does the Examiner ever provide a concrete example of such a situation. The Examiner does not assert that the theorized initialization situation would cause

the Wang server to compute an authorization code from a master code. With all due respect, this alleged motivation to modify Wang is unsupported by the cited art, and thus, is pure speculation.

Besides, modifying Wang as asserted by the Examiner fails to remedy the fact that Wang does not teach or suggest a central controller that computes an authorization code from a master code stored in its memory, and transmits the authorization code to a wireless communications device. That is, if Wang were to incorporate this nebulous "initialization situation" as the Examiner contends it can, there is no evidence whatsoever that it would cause the Wang server to compute and transmit the claimed authentication code.

Wang fails to teach or suggest claim 36. In addition, Wang cannot be modified as the Examiner contends. Nor has the Examiner provided a legally sufficient motivation to modify Wang. Accordingly, the §103 rejection of claim 36 fails as a matter of law.

F. The patent to Wang does not render claim 72 obvious under §103.

Claim 72 is directed to a device for issuing authorization code to activate or enable a protected function. In claim 72, the device computes an authorization code based on a master code stored in its memory. The device then transmits the authorization code to a wireless communications device. For the Board's convenience, claim 72 appears below in its entirety.

> 72. A device for issuing authorization code to activate or enable a protected function, said device comprising:
> memory to store a master code;
> an interface to communicate with a wireless communication device;
> a processor programmed to:
> compute an authorization code based on said master code in response to receipt of an initialization request from said wireless communication device;
> transmit said authorization code to said wireless communication device.

The Wang patent does not teach a device having a processor that computes an authorization code from a master code stored in its memory. Instead, Wang teaches a server

that provides a user's PEAD with an executable computer program called a TP. As noted above, the TP executes predetermined functionality that allows a user to approve a particular electronic transaction. The TP is not an authentication code, nor does it include an authorization code. Moreover, Wang never suggests that it does.

In addition, Wang fails to teach or suggest that the disclosed server computes an authentication code responsive to receiving an initialization request from the wireless communications device. Nor does Wang teach or suggest that the server stores a master code from which the authorization code is computed. Applicants note that the Examiner has failed to provide any proof that Wang teaches or suggests a master code. Rather, the entire rejection is a recitation of the claim language supported by the "Brief Summary" section of the Wang patent. Neither this section nor the remainder of the Wang patent teaches or suggests that the server stores a master code.

Finally, the Examiner proffers the same *legally insufficient* motivation to modify Wang as that stated above for claim 36. As such, the motivation to modify Wang also fails with respect to claim 72. Simply put, Wang fails to teach or suggest claim 72, and it cannot be modified as the Examiner asserts to render claim 72 obvious. Moreover, the alleged motivation to modify Wang is legally insufficient and, thus, cannot credibly support a § 103 rejection. Accordingly, the §103 rejection of claim 72 fails as a matter of law.

G. The Examiner has failed to put forth a legally sufficient prima facie case of obviousness regarding claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71.

The Examiner rejected claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71. First, each of these claims depends directly or indirectly from an independent claim that is patentable over the cited art. Therefore, these claims include all the limitations of their respective independent claim. It necessarily follows that because their respective independent claims are patentable, claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71 are also patentable over the cited art.

In addition, however, the Examiner's support of the rejections to the dependent claims cannot withstand legal scrutiny. Particularly, the Examiner appears to include claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71 in the §103 rejection over Henderson. *Final Office Action*, p. 3, ¶2. However, the Examiner never provides any proof (e.g., a cited passage in Henderson) to support the rejection of any of these claims. The only discussion of claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71 by the Examiner is an unsupported assertion that the "particular features [of these claims] are well known in the art for the purpose of handling information across processing systems and for the purpose of security." *Final Office Action*, p. 4, ¶3. That is the extent to which the Examiner supports the rejection of these claims. The Examiner does not attempt to qualify this theory, or provide evidence to support the assertions. Rather, the Examiner merely states that because these features are well known, they must be obvious.

With respect to independent claim 1:

G1. Claim 2

The Examiner did not provide any evidence to prove that it is known in the art to generate an authorization code based on a combination of a secret code and a time indication to limit access to a protected function to a defined time period.

> 2. The method of claim 1 wherein storing an authorization code in said wireless communication device comprises generating an authorization code based on a combination of a secret code and a time indication to limit access to said protected function to a defined time period.

G2. Claim 3

The Examiner did not provide any evidence to prove that it is known in the art to generate an authorization code by further combining a device identifier associated with the access control device with the secret code and the time indication.

> 3. The method of claim 2 wherein generating an authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

G3. Claim 4

The Examiner did not provide any evidence to prove that it is known in the art to store a plurality of authorization codes in the wireless communication device, wherein each of the authorization codes is associated with a different time period.

> 4. The method of claim 2 wherein storing an authorization code in said wireless communication device comprises storing a plurality of authorization codes in said wireless communication device, each said authorization code being associated with a different time period.

G4. Claim 6

The Examiner did not provide any evidence to prove that it is known in the art for a wireless communication device to transmit, to the access control device, an access request that includes a device identifier associated with the access control device.

> 6. The method of claim 1 wherein transmitting an access request from said wireless communication device to an access control device comprises transmitting a device identifier associated with said access control device to said access control device.

G5. Claim 7

The Examiner did not provide any evidence to prove that it is known in the art for a wireless communication device to further include a group identifier derived from the device identifier in the access request transmitted to the access control device.

> 7. The method of claim 6 wherein transmitting a device identifier associated with said access control device to said access control device comprises transmitting a group identifier derived from said device identifier.

G6. Claim 8

The Examiner did not provide any evidence to prove that it is known in the art to compute an authentication response based on the authentication challenge and the authorization code by combining selected portions of the authentication challenge and the authorization code with a non-reversible function.

> 8. The method of claim 1 wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining selected portions of said authentication challenge and said authorization code with a non-reversible function.

G7. Claim 9

The Examiner did not provide any evidence to prove that it is known in the art for the authentication challenge to include at least a random number, and that the random number is the selected portion of the authentication challenge that is combined with the authorization code to compute the authentication response.

> 9. The method of claim 1 wherein said authentication challenge includes at least a random number and wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining said random number of said authentication challenge and said authorization code.

G8. Claim 10

The Examiner did not provide any evidence to prove that it is known in the art to compute the authentication response by combining a device identifier associated with the access control device with the random number of the authentication challenge and the authorization code.

> 10. The method of claim 9 wherein computing an authentication response based on said authentication challenge and said authorization code further comprises combining a device identifier associated with said access control device with said random number of said authentication challenge and said authorization code.

G9. Claim 12

The Examiner did not provide any evidence to prove that it is known in the art for the wireless communications device to transmit an electronic identity to a central controller, and to receive the authorization code once the central controller has verified the electronic identity.

> 12. The method of claim 1 further comprising transmitting electronic identity from said wireless communication device to a central controller and receiving said authorization code from said central controller following verification of said electronic identity.

G10. Claim 13

The Examiner did not provide any evidence to prove that it is known in the art for the electronic identity of claim 12 to be a credit identity of a user verified by a credit agency.

> 13. The method of claim 12 wherein said electronic identity is a credit identity of a user verified by a credit agency.

With respect to independent claim 15:

G11. Claim 16

The Examiner did not provide any evidence to prove that it is known in the art to store the authorization code that is used to generate the expected response in the access control device.

> 16. The method of claim 15 further comprising storing said authorization code in said access control device.

G12. Claim 17

The Examiner did not provide any evidence to prove that it is known in the art to store a plurality of authorization codes in the access control device, wherein each of the authorization codes valid for a defined time period.

> 17. The method of claim 16 wherein storing said authorization code in said access control device comprises storing a plurality of authorization codes in said access control device, each authorization code being valid for a defined time period.

G13. Claims 18, 19

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to compute the authorization code based on a combination of a secret code and a time indication.

> 18. The method of claim 15 further comprising computing said authorization code based on a combination of a secret code and a time indication.
>
> 19. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by said access control device.

G14. Claim 20

The Examiner did not provide any evidence to prove that it is known in the art for the central controller in communication with the access control device to compute the authorization code based on a combination of a secret code and a time indication.

> 20. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by a central controller in communication with said access control device.

G15. Claim 21

The Examiner did not provide any evidence to prove that it is known in the art to compute the authorization code by combining a device identifier associated with the access control device with the secret code and the time indication.

> 21. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

G16. Claim 22

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to receive a device identifier associated with the access control device, and to transmit the authentication challenge only if the access control device receives the correct device identifier.

> 22. The method of claim 15 wherein said access request includes a device identifier to address said access control device, and wherein said method further comprises reading said device identifier and transmitting said authentication challenge only if a correct device identifier is received by said access control device.

G17. Claims 23, 24

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to compute the authentication challenge.

> 23. The method of claim 15 further comprising computing said authentication challenge.
>
> 24. The method of claim 23 wherein computing said authentication challenge is performed by said access control device.

G18. Claim 25

The Examiner did not provide any evidence to prove that it is known in the art for a central controller in communication with the access control device to compute the authentication challenge.

> 25. The method of claim 23 wherein computing said authentication challenge is performed by a central controller in communication with said access control device.

G19. Claim 26

The Examiner did not provide any evidence to prove that it is known in the art to compute the authentication challenge by generating a random number.

> 26. The method of claim 23 wherein computing said authentication challenge comprises generating a random number.

G20. Claim 27

The Examiner did not provide any evidence to prove that it is known in the art to compute the authentication challenge by combining the random number with a time indication.

> 27. The method of claim 26 wherein computing said authentication challenge comprises combining said random number with a time indication.

G21. Claim 28

The Examiner did not provide any evidence to prove that it is known in the art to compute the expected authentication response.

> 28. The method of claim 15 further comprising computing said expected authentication response.

G22. Claim 29

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to compute the expected authentication response.

> 29. The method of claim 28 wherein computing said expected authentication response is performed by said access control device.

G23. Claim 30

The Examiner did not provide any evidence to prove that it is known in the art for a central controller in communication with the access control device to compute the expected authentication response.

> 30. The method of claim 28 wherein computing said expected authentication response is performed by a central controller in communication with said access control device.

G24. Claim 31

The Examiner did not provide any evidence to prove that it is known in the art to compute the expected authentication response by combining selected portions of the authentication challenge and the authorization code.

> 31. The method of claim 28 wherein computing said expected authentication response comprises combining selected portions of said authentication challenge and said authorization code.

G25. Claim 32

The Examiner did not provide any evidence to prove that it is known in the art to compute the expected authentication response by combining a device identifier associated with the access control device with the selected portions of the authentication challenge and the authorization code.

> 32. The method of claim 31 wherein computing said expected authentication response further comprises combining a device identifier associated with said access control device with said selected portion of said authentication challenge and said authorization code.

G26. Claim 33

The Examiner did not provide any evidence to prove that it is known in the art to compute the expected authentication response by combining at least a random number included in the authentication challenge with the authorization code.

> 33. The method of claim 31 wherein said authentication challenge includes at least a random number and where combining selected portions of said authentication challenge and said authorization code comprises combining said random number with said authorization code.

G27. Claim 34

The Examiner did not provide any evidence to prove that it is known in the art to compute the expected authentication response by combining the selected portions of the authentication challenge and the authorization code using a non-reversible function.

> 34. The method of claim 31 wherein combining selected portions of said authentication challenge and said authorization code comprises combining said selected portions of said authentication challenge and said authorization code using a non-reversible function.

With respect to independent claim 40:

G28. Claim 41

The Examiner did not provide any evidence to prove that it is known in the art for the authentication code to be based on a master code.

> 41. The device of claim 40 wherein said authorization code is based on a master code.

G29. Claim 42

The Examiner did not provide any evidence to prove that it is known in the art for the authentication code to comprise a combination of the master code and a time indication to limit access to said protected function to a defined time period.

> 42. The device of claim 41 wherein said authorization code comprises a combination of said master code and a time indication to limit access to said protected function to a defined time period.

G30. Claim 43

The Examiner did not provide any evidence to prove that it is known in the art for the wireless communications device to store a plurality of authorization codes for a plurality of defined time periods.

> 43. The device of claim 42 wherein said memory stores a plurality of authorization codes for a plurality of defined time periods.

G31. Claim 44

The Examiner did not provide any evidence to prove that it is known in the art for the authorization code to comprise a combination of the master code and the identification code associated with the protected function.

> 44. The device of claim 41 wherein said authorization code comprises a combination of said master code with identification code associated with said protected function.

G32. Claim 45

The Examiner did not provide any evidence to prove that it is known in the art for the identification code associated with the protected function to uniquely identify the protected function.

> 45. The device of claim 44 wherein said identification code uniquely identifies said protected function.

G33. Claim 46

The Examiner did not provide any evidence to prove that it is known in the art for the identification code to comprise a plurality of symbols, wherein a subset of the symbols identifies a group of access control devices.

> 46. The device of claim 45 wherein said identification code comprises a plurality of symbols and wherein a subset of said symbols identifies a group of access control devices.

G34. Claim 54

The Examiner did not provide any evidence to prove that it is known in the art for the wireless communications device to include a processor that combines selected portions of the authentication challenge with the authorization code to generate the authentication response.

> 54. The device of claim 40 wherein said processor combines selected portions of said authentication challenge with said authorization code to generate said authentication response.

G35. Claim 55

The Examiner did not provide any evidence to prove that it is known in the art for the processor to generate the authentication response by combining the selected portions of the authentication challenge with the authorization code and an identification code associated with the protected function.

> 55. The device of claim 54 wherein said processor further combines said selected portions of said authentication challenge and said authorization code with an identification code associated with said protected function to generate said authentication response.

G36. Claim 56

The Examiner did not provide any evidence to prove that it is known in the art for the processor to generate the authentication response by combining the selected portions of the authentication challenge with the authorization code, wherein the selected portions of the authentication challenge includes at least a random number.

> 56. The device of claim 54 wherein said selected portions of said authentication challenge includes at least a random number contained in said authentication challenge.

With respect to independent claim 60:

G37. Claim 61

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to include a processor that computes the authorization code based on a master code stored in its memory.

> 61. The access control device of claim 60 further comprising memory to store a master code, said processor being further programmed to compute said authorization code based on said master code.

G38. Claim 62

The Examiner did not provide any evidence to prove that it is known in the art for the processor to compute the authorization code by combining the master code with a time indication associated with a time period during which the authorization code is valid.

> 62. The access control device of claim 61 wherein said processor computes said authorization code by combining said master code with a time indication associated with a time period during which said authorization code is valid.

G39. Claim 63

The Examiner did not provide any evidence to prove that it is known in the art for the processor to compute the authorization code by further combining a device identifier with the master code and the time indication.

> 63. The access control device of claim 62 wherein said processor computes said authorization code by further combining a device identifier with said master code and said time indication.

G40. Claim 64

The Examiner did not provide any evidence to prove that it is known in the art for the access control device to further comprise a tamper resistant security module containing memory in which the master code is stored.

> 64. The access control device of claim 62 further comprising a tamper resistant security module containing said memory.

G41. Claims 65, 67

The Examiner did not provide any evidence to prove that it is known in the art for the authentication challenge to comprise a random bit pattern and a time indication.

> 65. The access control device of claim 60 wherein said authentication challenge comprises a random bit pattern.

> 67. The access control device of claim 65 wherein said authentication challenge generated by said processor further comprises a time indication.

Indeed, the Examiner bases the rejection of each of these claims on mere speculation on what is known in the art. The Examiner never articulates a rationale that suggests to one skilled in the art that it would be desirable or advantageous to modify Henderson with the alleged known features of any of the rejected dependent claims. The Examiner certainly never provides any concrete evidence of record to support the assertions. Rather, the Examiner simply makes a conclusory statement that because the subject matter is (allegedly) known in the art, the Henderson system could be modified to use it. However, "[t]he question of motivation is material to patentability, and cannot be based on a subjective belief and unknown authority." *In re Lee*, 61 U.S.P.Q. 2d 1430,1434 (Fed. Cir. 2002) (emphasis added). Moreover, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon* 733 F.2d 900, 902, 221 U.S.P.Q. 1125 (Fed. Cir. 1984) (emphasis added).

A motivation to modify a reference based on mere speculation is legal error and cannot stand. Neither Henderson nor Wang teaches or suggests claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71, and notably, the Examiner never asserts that they do. Moreover, the Examiner has yet to provide proof of whatever prior art teaches or suggests any of claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71, even after Applicants explicitly requested such proof in Applicants' September 2, 2005 response. Therefore, the §103 rejection of claims 2-4, 6-11, 15-35, 40-50, 54-56, and 60-71 fails as a matter of law.

H. Nether Henderson nor Wang, alone or in combination, render claims 5, 12-14, 51-53, and 57-59 obvious under §103.

The Examiner rejected claims 5, 12-14, 51-53, and 57-59 as being unpatentable under §103 over Henderson in view of Wang. However, each of claims 5, 12-14, 51-53, and 57-59 depend directly or indirectly from an independent claim that is patentable over the cited

references. Therefore, the dependent claims 5, 12-14, 51-53, and 57-59 are also necessarily patentable over the cited references.

In addition, the rejection of these claims is unsupported by the Examiner, and unsupported by the cited references. Particularly, the Examiner merely states that "Henderson teaches as noted above. ... Henderson does not teach such e-transactions...[but Wang does] for ease of commerce." *Final Office Action*, p. 4, ¶5-8. As such, the Examiner theorizes that it would be obvious to modify Henderson with Wang. Henderson teaches a system that facilitates obtaining access to a door key to gain entry to a house. Wang discloses security for electronic transactions. Whether Wang teaches e-transactions means nothing. The two references are completely unrelated, and one skilled in the art would never look to one to modify the other.

Further, the alleged motivation to combine the references – i.e., for the ease of commerce – has absolutely nothing to do with obtaining a door key from a lockbox system. It only relates to electronic transaction systems, which Wang already teaches. The Henderson lockboxes are not used in e-commerce – indeed, they are not used to purchase anything. Likewise, the Wang system (i.e., POS, ATM systems) are not used to secure real estate lockboxes, and Wang never suggests that they can be used for such a purpose. Therefore, it is unclear how modifying the lockbox system of Henderson with the "e-transactions" of Wang would be desirable for Henderson, or how Wang would operate with the Henderson system to render claims 5, 12-14, 51-53, and 57-59 obvious. The Examiner never addresses these issues. Indeed, it appears as though the rejections to claims 5, 12-14, 51-53, and 57-59 are based on impermissible hindsight reconstruction. As the Board is aware, this is never allowed.

Neither Henderson nor Wang teach or suggest, alone or in combination, any of claims 5, 12-14, 51-53, and 57-59. Moreover, the references cannot be combined, and even if they could, they do not teach or suggest any of claims 5, 12-14, 51-53, and 57-59. Thus, the §103 rejection to claims 5, 12-14, 51-53, and 57-59 fails as a matter of law.

In conclusion, the Examiner has failed to establish a legally sufficient prima facie case of obviousness with respect to any of the pending claims 1-77 for at least the reasons stated above. Therefore, all the §103 rejections fail as a matter of law. Applicants respectfully request that the Board reverse all §103 rejections.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: November 7, 2005

Stephen A. Herrera
Registration No.: 47,642

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844
Facsimile: (919) 854-2084

(VIII.) CLAIMS APPENDIX

1. A method of enabling or activating a protected function, said method comprising:

storing an authorization code in a wireless communication device;

transmitting an access request from said wireless communication device to an access control device;

receiving an authentication challenge from said access control device at said wireless communication device in response to said access request;

computing an authentication response based on said authentication challenge and said authorization code; and

transmitting said authentication response from said wireless communication device to said access control device.

2. The method of claim 1 wherein storing an authorization code in said wireless communication device comprises generating an authorization code based on a combination of a secret code and a time indication to limit access to said protected function to a defined time period.

3. The method of claim 2 wherein generating an authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

4. The method of claim 2 wherein storing an authorization code in said wireless communication device comprises storing a plurality of authorization codes in said wireless communication device, each said authorization code being associated with a different time period.

5. The method of claim 1 wherein storing an authorization code in said wireless communication device comprises storing said authorization code in a smart card associated with said wireless communication device.

6. The method of claim 1 wherein transmitting an access request from said wireless communication device to an access control device comprises transmitting a device identifier associated with said access control device to said access control device.

7. The method of claim 6 wherein transmitting a device identifier associated with said access control device to said access control device comprises transmitting a group identifier derived from said device identifier.

8. The method of claim 1 wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining selected portions of said authentication challenge and said authorization code with a non-reversible function.

9. The method of claim 1 wherein said authentication challenge includes at least a random number and wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining said random number of said authentication challenge and said authorization code.

10. The method of claim 9 wherein computing an authentication response based on said authentication challenge and said authorization code further comprises combining a device identifier associated with said access control device with said random number of said authentication challenge and said authorization code.

11. The method of claim 1 wherein protected function is unlocking a door.

12. The method of claim 1 further comprising transmitting electronic identity from said wireless communication device to a central controller and receiving said authorization code from said central controller following verification of said electronic identity.

13. The method of claim 12 wherein said electronic identity is a credit identity of a user verified by a credit agency.

14. The method of claim 12 wherein transmitting electronic identity from said wireless communication device to a central controller comprises transmitting said electronic identity to said central controller via a wireless communication interface.

15. A method of enabling or activating a protected function, said method comprising:

receiving an access request from a wireless communication device at an access control device;

transmitting an authentication challenge from said access control device to said wireless communication device in response to said access request;

receiving an authentication response based on said authentication challenge and an authorization code;

comparing said received authentication response with an expected authentication response; and

generating a control signal to permit access to said protected function if said received authentication response matches said expected authentication response.

16. The method of claim 15 further comprising storing said authorization code in said access control device.

17. The method of claim 16 wherein storing said authorization code in said access control device comprises storing a plurality of authorization codes in said access control device, each authorization code being valid for a defined time period.

18. The method of claim 15 further comprising computing said authorization code based on a combination of a secret code and a time indication.

19. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by said access control device.

20. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by a central controller in communication with said access control device.

21. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

22. The method of claim 15 wherein said access request includes a device identifier to address said access control device, and wherein said method further comprises reading said device identifier and transmitting said authentication challenge only if a correct device identifier is received by said access control device.

23. The method of claim 15 further comprising computing said authentication challenge.

24. The method of claim 23 wherein computing said authentication challenge is performed by said access control device.

25. The method of claim 23 wherein computing said authentication challenge is performed by a central controller in communication with said access control device.

26. The method of claim 23 wherein computing said authentication challenge comprises generating a random number.

27. The method of claim 26 wherein computing said authentication challenge comprises combining said random number with a time indication.

28. The method of claim 15 further comprising computing said expected authentication response.

29. The method of claim 28 wherein computing said expected authentication response is performed by said access control device.

30. The method of claim 28 wherein computing said expected authentication response is performed by a central controller in communication with said access control device.

31. The method of claim 28 wherein computing said expected authentication response comprises combining selected portions of said authentication challenge and said authorization code.

32. The method of claim 31 wherein computing said expected authentication response further comprises combining a device identifier associated with said access control device with said selected portion of said authentication challenge and said authorization code.

33. The method of claim 31 wherein said authentication challenge includes at least a random number and where combining selected portions of said authentication challenge and said authorization code comprises combining said random number with said authorization code.

34. The method of claim 31 wherein combining selected portions of said authentication challenge and said authorization code comprises combining said selected portions of said authentication challenge and said authorization code using a non-reversible function.

35. The method of claim 15 wherein said protected function is unlocking a door.

36. A method of programming a wireless communication device with an authorization code used to enable or activate a protected function, said method comprising:

storing a master code in a central controller;

receiving an initialization request from said wireless communication device;

computing an authorization code based on said master code at said central controller in response to receipt of said initialization request;

communicating said authorization code to said wireless communication device.

37. The method of claim 36 further comprising storing said authorization code in said wireless communication device.

38. The method of claim 36 wherein storing a master code in a central controller comprises storing said master code in a tamper-resistant security module.

39. The method of claim 36 wherein said initialization request includes an electronic identity of the requesting party and wherein said method further comprises authenticating the electronic identity of the requesting party.

40. A device for enabling or activating a protected function, said device comprising:

memory to store an authorization code;

a wireless transmitter to transmit an access request and an authentication response to an access control device;

a wireless receiver to receive an authentication challenge from said access control device responsive to said access request;

a processor to compute said authentication response based on said authentication challenge received from said access control device and said authorization code.

41. The device of claim 40 wherein said authorization code is based on a master code.

42. The device of claim 41 wherein said authorization code comprises a combination of said master code and a time indication to limit access to said protected function to a defined time period.

43. The device of claim 42 wherein said memory stores a plurality of authorization codes for a plurality of defined time periods.

44. The device of claim 41 wherein said authorization code comprises a combination of said master code with identification code associated with said protected function.

45. The device of claim 44 wherein said identification code uniquely identifies said protected function.

46. The device of claim 45 wherein said identification code comprises a plurality of symbols and wherein a subset of said symbols identifies a group of access control devices.

47. The device of claim 40 wherein said protected function is the ability to unlock a door and wherein said authorization code unlocks said door.

48. The device of claim 40 wherein said wireless transmitter is a short-range wireless transmitter.

49. The device of claim 48 wherein said wireless receiver is a short-range wireless receiver.

50. The device of claim 49 wherein said wireless transmitter and said wireless receiver comprise a BLUETOOTH transmitter and BLUETOOTH receiver respectively.

51. The device of claim 40 further comprising a cellular radiotelephone transceiver for communicating with a mobile communication network.

52. The device of claim 40 further comprising a tamper-resistant security module containing said processor.

53. The device of claim 52 wherein said tamper resistant security module comprises a smart card.

54. The device of claim 40 wherein said processor combines selected portions of said authentication challenge with said authorization code to generate said authentication response.

55. The device of claim 54 wherein said processor further combines said selected portions of said authentication challenge and said authorization code with an identification code associated with said protected function to generate said authentication response.

56. The device of claim 54 wherein said selected portions of said authentication challenge includes at least a random number contained in said authentication challenge.

57. The device of claim 40 wherein said device exchanges messages with a central controller according to a predetermined protocol to obtain said authorization code.

58. The device of claim 57 wherein said device transmits its identity to said central controller as part of said predetermined protocol to enable its identity to be authenticated by said central controller.

59. The device of claim 58 wherein said identity is the credit identity of a user verified by a credit agency.

60. An access control device to secure a protected function, said access control device comprising:

a wireless transceiver to communicate with a wireless communication device;

a processor programmed to:

generate an authentication challenge in response to an access request from said wireless communication device;

transmit said authentication response via said wireless transceiver to said wireless communication device;

receive an authentication response from said wireless communication device via said wireless transceiver;

compare said received authentication response to an expected authentication response based on said authentication challenge and an authorization code; and

generate a control signal to permit access to said protected function if said expected authentication response matches said received authentication response.

61. The access control device of claim 60 further comprising memory to store a master code, said processor being further programmed to compute said authorization code based on said master code.

62. The access control device of claim 61 wherein said processor computes said authorization code by combining said master code with a time indication associated with a time period during which said authorization code is valid.

63. The access control device of claim 62 wherein said processor computes said authorization code by further combining a device identifier with said master code and said time indication.

64. The access control device of claim 62 further comprising a tamper resistant security module containing said memory.

65. The access control device of claim 60 wherein said authentication challenge comprises a random bit pattern.

66. The access control device of claim 64 further comprising a random bit generator to generate said random bit pattern.

67. The access control device of claim 65 wherein said authentication challenge generated by said processor further comprises a time indication.

68. The access control device of claim 60 further comprising an actuator responsive to said control signal to unlock a door.

69. The access control device of claim 60 wherein said access control device is identified by a device identifier and wherein said processor is programmed to respond to access requests containing at least a portion of said device identifier.

70. The access control device of claim 60 further comprising a clock to provide a time indication to said processor to use to validate an authentication response.

71. The access control device of claim 70 wherein said processor is responsive to a reset command to reset said clock to a time indicated in said reset command.

72. A device for issuing authorization code to activate or enable a protected function, said device comprising:

memory to store a master code;

an interface to communicate with a wireless communication device;

a processor programmed to:

compute an authorization code based on said master code in response to receipt of an initialization request from said wireless communication device;

transmit said authorization code to said wireless communication device.

73. The device of claim 72 further comprising a tamper resistant security module containing said memory to hinder extraction of said master code from said memory.

74. The device of claim 72 wherein said interface is a wireless interface.

75. The device of claim 74 wherein said interface is a wireless BLUETOOTH interface.

76. The device of claim 75 wherein said processor is programmed to execute an authentication procedure in response to receipt of said initialization request.

77. The device of claim 76 wherein said processor authenticates a claimed electronic identity received from said wireless communication device as part of said authentication procedure.

(IX.) EVIDENCE APPENDIX

There is no further evidence not contained in the prosecution history.

(X.) RELATED PROCEEDINGS APPENDIX

There are no related proceedings.

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818)

FEE TRANSMITTAL For FY 2005

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 500

Complete if Known	
Application Number	09/862,879
Filing Date	May 22, 2001
First Named Inventor	DENT
Examiner Name	Jung, David Yiuk
Art Unit	2134
Attorney Docket Number	P12563-US1 4015-844

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: _____ Deposit Account _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIMS FEE

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	X _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	X _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____	/ 50 = _____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fee Paid ($)
Filing of Appeal Brief	500

SUBMITTED BY			
Signature		Registration No. (Attorney/Agent) 47,642	Telephone (919) 854-1844
Name (Print/Type) Stephen A. Herrera			Date November 7, 2005